**SOFTWARE SETUP**

**Required Tool:**

* First Install Node.js with this URL: [nodejs.org](https://nodejs.org/) install Latest version of node js.
* Then Install XAMPP for creating local server with this URL: [www.apachefriends.org](https://www.apachefriends.org/) according to your OS Setup.

**Program File Setup:**

* **Frontend Setup:**
* First download the attached frontend code.
* Then open that project file in any IDE (integrated development environment) application (Visual Studio is preferable)
* Then open terminal and type this command to install node module to get all packages.



* If it doesn’t install properly force to install the node module with this command.



* Give your credentials in frontend .env file.



* **Backend Setup:**
* First download the attached backend code.
* Then open that project file in any IDE (integrated development environment) application (Visual Studio is preferable)
* Then open terminal and type this command to install node module to get all packages.



* If it doesn’t install properly force to install the node module with this command.



* Give your credentials in backend .env file.



* **Database Setup:**
* First create your own data base for your project in XAMPP server.
* Then import the attached SQL file into your database
* The if you want to customize the DB structure you can edit those things

**After all Frontend and Backend setup**

* Open Terminal in both frontend and backend type this command to start our project.



**AWS Server Setup**

**Steps for S3 Bucket Setup:**

**Step 1:**

* Sign in to AWS Console
* Go to the AWS Management Console ([aws.a HYPERLINK "https://aws.amazon.com/"m HYPERLINK "https://aws.amazon.com/"az HYPERLINK "https://aws.amazon.com/"o HYPERLINK "https://aws.amazon.com/"n HYPERLINK "https://aws.amazon.com/".c HYPERLINK "https://aws.amazon.com/"o HYPERLINK "https://aws.amazon.com/"m](https://aws.amazon.com/)).
* Sign in with your AWS account credentials.

**Step 2:**

* Access S3 Once logged in, search for "S3" in the AWS services search bar and select "S3" under "Storage."

**Step 3:**

* Create a New Bucket in the S3 dashboard, click the "Create bucket" button.

**Step 4:**

* Configure the Bucket Name: Choose a globally unique name for your bucket. It must be lowercase and follow DNS naming conventions.
* Region: Select the AWS region where you want to create the bucket. Choose a region that is geographically closest to your users.
* Configure options: You can leave this section as default or configure advanced settings like versioning, logging, and tags as needed.

**Step 5:**

* Set Permissions Block Public Access: By default, S3 buckets are private. Configure block public access settings according to your requirements.
* Bucket Policy: You can attach a bucket policy to specify who can access the bucket and what actions they can perform.
* Access Control List (ACL): Set permissions at the object level using ACLs if necessary.

**Step 6:**

* Review your bucket configuration settings to ensure they are accurate.
* Click the "Create bucket" button.

**Step 7:**

* Once your bucket is created, you can access it by clicking on its name in the S3 dashboard.

**Step 8:**

* Access IAM once logged in, search for "IAM" (Identity and Access Management) in the AWS services search bar and select "IAM" under "Security, Identity, & Compliance."

**Step 9:**

* Create or Select a User. If you haven't already created an IAM user, you can do so by navigating to "Users" in the IAM dashboard and clicking "Add user." Follow the prompts to create the user with the desired permissions.
* If you already have an IAM user you want to generate a secret key for, select that user by clicking on their name.

**Step 10:**

* Generate Secret Access Key. In the user details page, navigate to the "Security credentials" tab.
* Under "Access keys," click "Create access key."
* A pop-up window will appear with the access key ID and secret access key. Click "Download .csv file" to save the access key information to your computer.

**Step 11:**

* Store the Access Key Securely. The secret access key is only displayed once during creation. Make sure to save it securely, as you won't be able to retrieve it again.
* If you lose the secret access key, you can create a new access key and deactivate the old one.

**Step 12:**

* Configure Permissions. Ensure that the IAM user has the necessary permissions to access the S3 bucket. This can be done by attaching the appropriate policy to the user. You might want to use an existing policy or create a custom one.

**Step 13:**

* Use the Access Key. You can now use the access key ID and secret access key to access AWS services, including S3, programmatically or through AWS CLI, SDKs, or other tools.
* When accessing S3, provide the access key credentials for authentication.
* The config the access key in backend code.

**Steps for Purchasing Server in AWS:**

**Step 1:**

* Sign in to AWS Console
* Go to the AWS Management Console ([aws.amazo HYPERLINK "https://aws.amazon.com/"n HYPERLINK "https://aws.amazon.com/".com](https://aws.amazon.com/)).
* Sign in with your AWS account credentials.

**Step 2:**

* Access EC2 Dashboard. Once logged in, search for "EC2" (Elastic Compute Cloud) in the AWS services search bar and select "EC2" under "Compute."

**Step 3:**

* Launch an Instance. In the EC2 dashboard, click the "Instances" link in the left navigation pane.
* Click the "Launch Instance" button to start the instance creation process.

**Step 4:**

* Choose an Amazon Machine Image (AMI). Select an Amazon Machine Image (AMI) to define the operating system and software for your server. You can choose from a variety of pre-configured AMIs, including those with different operating systems and applications.

**Step 5:**

* Choose an Instance Type. Select the instance type that matches your workload requirements. Instance types vary in terms of CPU, memory, storage, and network performance.

**Step 6:**

* Configure Instance Details. Configure instance details such as the number of instances, network settings, and IAM role (if applicable).

**Step 7:**

* Add Storage. Define the amount and type of storage (EBS volumes) required for your server. You can also configure additional storage options like encryption.

**Step 8:**

* Configure Security Groups. Configure security groups to control inbound and outbound traffic to your instance. You can define rules to allow specific types of traffic, such as SSH or HTTP.

**Step 9:**

* Review and Launch. Review your instance configuration to ensure it meets your requirements.
* Click the "Launch" button to proceed.

**Step 10:**

* Create or Use an Existing Key Pair. If you already have an SSH key pair, select it. If not, you can create a new key pair.
* Download and securely store the private key file (.pem). You'll need it to connect to your server.

**Step 11:**

* Launch the Instance. Click the "Launch Instances" button to create your EC2 instance.
* Your instance will start provisioning. You can monitor its status in the EC2 dashboard.

**Step 12:**

* Access Your Server. Once the instance is running, you can access it via SSH for Linux instances or Remote Desktop Protocol (RDP) for Windows instances.
* Use the private key file (.pem) for Linux or the provided password for Windows to connect securely.